ABSTRACT

A method, system, and computer program product for establishing security parameters that are used to exchange data on a secure connection. A piggy-backed key exchange protocol is defined, with which these security parameters are advantageously exchanged. By piggy-backing the key exchange onto other already-required messages (such as a client's HTTP GET request, or the server's response thereto), the overhead associated with setting up a secure browser-to-server connection is minimized. This technique is defined for a number of different scenarios, where the client and server may or may not share an encoding scheme, and is designed to maintain the integrity of application layer communication protocols. In one scenario, a client requests a server to propose a message encoding scheme. If the client has security-sensitive data to transmit with its request, it waits for the proposed scheme before sending this sensitive data to the server. Otherwise, the server may inform the client of the message encoding scheme in the same transmission used to send a response to a client's request.